IBM dashDB

Except as noted below, the terms of the IBM Bluemix Service Description or Terms of Use, as applicable, apply.

1. **Cloud Service Description**
   The following IBM Cloud Services are covered by this Cloud Service Description:
   a. IBM dashDB Entry
   b. IBM dashDB Enterprise
      (1) IBM dashDB Enterprise 64.1
      (2) IBM dashDB Enterprise 256.4
      (3) IBM dashDB Enterprise 256.12
   c. IBM dashDB Enterprise MPP.4

   IBM dashDB is a managed service which assists in the development of online analytical application processing. The service includes a database that stores user data in a structured format. This database can be accessed and modeled according to the user’s requirements through the service’s console. The service’s console allows users to create tables, load data into the tables and query the data loaded by the user. Tools and environments to help develop, store and share analytical reports are included with the service. The service includes samples and documentation to help create the online analytical applications.

   IBM dashDB Enterprise MPP is a clustered configuration of the IBM dashDB service, comprising a set of independent database nodes managed together as a single system. Database operations are parallel processed across all the database nodes. IBM will configure the associated nodes into one cluster.

2. **Security Description**
   In addition to the Security Description section of the IBM Bluemix Service Description or Terms of Use, as applicable, the following apply to IBM dashDB Enterprise and IBM dashDB Enterprise MPP.

   2.1 **User Management**
      When the Cloud Service is provisioned, a single administrative user is created for Client. The dashDB console provides administrative users the ability to create additional users. Those users may be defined with either administrative (“bluadmin”) access or regular (“bluuser”) access. Client is wholly responsible for managing the users defined via the console and the level of access assigned to them.

   2.2 **Direct access to the Cloud Services data store**
      Both administrative and regular users are able to directly access the Cloud Service data store using IBM DB2 client programs run outside the Bluemix environment. Client is wholly responsible for ensuring that such access is secured according to Client’s requirements. For example, Client may configure the clients such that SSL is used to protect network traffic.

   2.3 **Table level access control**
      The Cloud Service allows Client to manage the access rights associated with some database objects, such as tables. Client is wholly responsible for assigning, managing and reviewing these access rights.

   2.4 **Audit Reports**
      The Cloud Service instances are monitored using IBM InfoSphere Guardium. Monitoring reports are made available to Client through the dashDB console. Client is wholly responsible for accessing and interpreting the reports to determine if the activity they reflect is authorized.

   2.5 **Encryption for data at rest**
      The Cloud Service databases are automatically encrypted. The encryption uses Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) mode with a 256 bits key. Also, database backup images are automatically compressed and encrypted. Backup images are encrypted using AES in CBC mode with 256 bit keys.
3. **Entitlement and Billing Information**

3.1 **Charge Metrics**

The Cloud Service is offered in accordance with the following charge metric:

**Instance** - An instance is access to a specific configuration of the Cloud Service. Client will be charged for each instance of the Cloud Service that is deployed during the billing period.

3.2 **Entitlement Requirements**

IBM dashDB Entry is made available on a “Free Tier” basis that incurs no charges up to the level stated in the catalog. Use above that level will incur charges on a Pay As You Go basis.

IBM dashDB Enterprise and IBM dashDB Enterprise MPP are made available on a Subscription basis. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period stated in Client's Proof of Entitlement (PoE) or Transaction Document.

For IBM dashDB Enterprise MPP, each cluster must comprise a minimum of three (3) nodes, and you must acquire one (1) Instance entitlement per node.

3.3 **Partial Monthly Charges**

Each Instance is billed on a monthly basis. Partial month deployment/usage will be pro-rated.

4. **Term and Renewal Options**

The following terms apply to IBM dashDB Enterprise and IBM dashDB Enterprise MPP:

4.1 **Term**

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. Client may increase their level of use of the Cloud Service during the term by contacting IBM or their IBM Business Partner, and the increase will be confirmed in a Transaction Document.

4.2 **Cloud Services Term Renewal Options**

The Transaction Document will specify which of the following applies to renewal of the Cloud Service term.

4.2.1 **Automatic Renewal**

Where renewal is automatic, the Cloud Service will automatically renew for a term specified in the Transaction Document (either a one year term or the same duration as the expiring term) unless Client has provided written termination at least 90 days prior to the term expiration date.

4.2.2 **Continuous Billing**

Where billing is continuous, Client will continue to have access to the Cloud Service following the end of the term and will be billed for usage on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, Client must provide 90 days written notice of cancellation. Client will be billed for any outstanding access charges through the end of the month of cancellation.

4.2.3 **Renewal Required**

Where the renewal type is specified as "terminate", the Cloud Service will terminate at the end of the term and Client access will end. To continue to use the Cloud Service beyond the term end date, Client must order a new subscription term.

5. **No Personal Health Information**

The Cloud Service is not designed to comply with HIPAA and may not be used for the transmission or storage of any Personal Health Information.

6. **Safe Harbor Framework**

The Cloud Service does not comply with the US-EU and US-Swiss Safe Harbor Frameworks.

7. **Beta Service Terms and Conditions**

If a Cloud Service is designated “beta” or “early release” (a “Beta Service”), the following terms apply to the Beta Service in addition to the Beta Service terms of the IBM Bluemix Service Description:
7.1 Confidentiality

Client agrees to treat the following as "IBM Confidential Information" regardless of whether they contain restrictive markings indicating the confidential nature thereof or have been identified as IBM Confidential Information prior to disclosure: (a) the Beta Service, (b) any information provided to Client by IBM with regard to the Beta Service including, but not limited to, Beta Service-related materials such as specifications, plans, trends, strategies, benchmarks, performance characteristics, comparisons and other assessments of the Beta Service, (c) any information related to Client’s access to the Beta Service including, but not limited to, passwords or other access codes, and (d) all data, feedback, suggestions and/or written materials that Client provides to IBM related to the Beta Service. Client is authorized to use the IBM Confidential Information for the purpose for which it was disclosed or otherwise for the benefit of IBM. Notwithstanding any other terms of this Agreement, Client agrees not to communicate, publish, disseminate or otherwise discuss with or disclose to any third party the IBM Confidential Information (including but not limited to articles, papers or other written materials pertaining to the IBM Confidential Information) prior to IBM making such IBM Confidential Information publicly available without a non-disclosure obligation.

Client agrees to use the same care and discretion to avoid disclosure of the IBM Confidential Information as Client uses with Client’s own similar information that Client does not wish to disclose, but in no event will such degree of care be less than reasonable care. Client’s obligations with respect to the IBM Confidential Information will continue for a period of two years from Client’s receipt of the IBM Confidential Information. Client agrees not to disclose to IBM any information that is considered confidential or proprietary to Client or any third party except under a signed, separate, written confidential agreement. Notwithstanding the existence of any confidentiality or other agreement Client may have with IBM pertaining to confidential information, the preceding paragraphs will govern the treatment of the IBM Confidential Information.